PQ of the CP

Andy Newton,
IETF 85 SIDR
Conspicuous Disclosure

• In the X.509 PKI world, it is quite common to embed pointers into the CertificatePolicy extension as a PolicyQualifier
  – The IETF’s RPKI Certificate Policy (CP) covers the RPKI as a whole
  – Each CA can have a Certification Practices Statement
AOL’s CPS Pointer

```plaintext
SEQUENCE {
  OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
  OCTET STRING, encapsulates {
    SEQUENCE {
      SEQUENCE {
        OBJECT IDENTIFIER '1 3 6 1 4 1 1066 1 1000 1 0 2 2'
        # aol specific OID
        SEQUENCE {
          SEQUENCE {
            OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
            IA5String
            'http://pki-info.aol.com/AOLMSPKI/index.html'
            # aol specific URI for their CPS
          } } } } } }
```
Digicert’s CPS Pointer

SEQUENCE {
  OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
  OCTET STRING, encapsulates {
    SEQUENCE {
      SEQUENCE {
        OBJECT IDENTIFIER '2 16 840 1 114412 1 3 0 1'
        SEQUENCE {
          OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
          IA5String 'http://www.digicert.com/ssl-cps-repository.htm'}
        SEQUENCE {
          OBJECT IDENTIFIER unotice (1 3 6 1 5 5 7 2 2)
          SEQUENCE { BMPString 'Any use of this Certificate constitutes acceptance of the DigiCert CP/CPS and the Relying Party Agreement which limit liability and are incorporated herein by reference.' } } } } } }
Just One Problem


This extension MUST be present and MUST be marked critical. It MUST include exactly one policy, as specified in the RPKICP [RFC6484]

• RFC 6487 is ambiguous on PolicyQualifiers
• Required one line fix to two of the validators
• A specification update is needed
  • Coming soon